

ALGEBRA HW 1

CLAY SHONKWILER

1. 0.3.8

Prove that the equation $a^2 + b^2 = 3c^2$ has no solutions in nonzero integers a , b and c .

Proof. Suppose there exist nonzero integers a_0 , b_0 and c_0 such that $a_0^2 + b_0^2 = 3c_0^2$. Then

$$a_0^2 + b_0^2 \equiv 3c_0^2 \pmod{4}$$

or

$$\overline{a_0}^2 + \overline{b_0}^2 = \overline{3c_0}^2$$

in $\mathbb{Z}/4\mathbb{Z}$. Now, in this group, all squares are of the form $\overline{0}$ or $\overline{1}$, meaning

$$\overline{a_0} = \overline{b_0} = \overline{c_0}.$$

Hence, a_0 , b_0 and c_0 are all divisible by 2. Dividing both sides of the original equation by 4, this means

$$\frac{a_0^2}{4} + \frac{b_0^2}{4} = 3\frac{c_0^2}{4}$$

so $\frac{a_0}{2}$, $\frac{b_0}{2}$, $\frac{c_0}{2} \in \mathbb{Z}$ are also solutions of the equation.

Using the above argument, we then see that

$$\frac{a_0}{4}, \frac{b_0}{4}, \frac{c_0}{4}$$

are also integer solutions of the original equation and that, in general, so are $\frac{a_0}{2^n}$, $\frac{b_0}{2^n}$ and $\frac{c_0}{2^n}$ for all $n \in \mathbb{N}$. However, if $N > a_0$,

$$\frac{a_0}{2^N} \notin \mathbb{Z},$$

a contradiction. Therefore, we conclude that there are no nonzero integer solutions of the equation $a^2 + b^2 = 3c^2$. \square

2. 0.3.13

Let $n \in \mathbb{Z}$, $n > 1$, and let $a \in \mathbb{Z}$ with $1 \leq a \leq n$. Prove that if a and n are relatively prime then there is an integer c such that $ac \equiv 1 \pmod{n}$.

Proof. Since a and n are relatively prime, we know that $(a, n) = 1$. Now, since the g.c.d. of two integers is a \mathbb{Z} -linear combination of the integers, there exist $c, d \in \mathbb{Z}$ such that

$$1 = ac + nd.$$

Subtracting nd from both sides, we see that

$$ac = 1 + n(-d),$$

or

$$ac \equiv 1 \pmod{n}.$$

□

3. 1.2.10

Let G be the group of rigid motions in \mathbb{R}^3 of a cube. Show that $|G| = 24$.

Let C denote the cube, and label the vertices of C by $1, 2, \dots, 8$ such that vertex 1 is adjacent to vertex 2. Now, if $\sigma \in G$, there are 8 possibilities for the value of $\sigma(1)$, the eight vertices of C . Furthermore, for each of the 8 possible values of $\sigma(1)$, there are three possibilities for where vertex 2 can be sent, the 3 vertices adjacent to $\sigma(1)$. Hence, there are $8 \cdot 3 = 24$ possible rigid motions of C , or $|G| = 24$.

4. 1.3.15

Prove that the order of an element in S_n equals the least common multiple of the lengths of the cycles in its cycle decomposition.

Proof. Let $\sigma \in S_n$ and let

$$\sigma = (a_1 a_2 \dots a_{m_1})(a_{m_1+1} a_{m_1+2} \dots a_{m_2}) \dots (a_{m_{k-1}+1} a_{m_{k-1}+2} \dots a_{m_k})$$

be the cycle decomposition of σ . Let n be an arbitrary positive integer. Since disjoint cycles commute, we see that

$$\begin{aligned} \sigma^n &= [(a_1 a_2 \dots a_{m_1})(a_{m_1+1} a_{m_1+2} \dots a_{m_2}) \dots (a_{m_{k-1}+1} a_{m_{k-1}+2} \dots a_{m_k})]^n \\ &= (a_1 a_2 \dots a_{m_1})^n (a_{m_1+1} a_{m_1+2} \dots a_{m_2})^n \dots (a_{m_{k-1}+1} a_{m_{k-1}+2} \dots a_{m_k})^n \end{aligned}$$

$\sigma^n = 1$ if and only if

$$(a_{m_{j-1}+1} a_{m_{j-1}+2} \dots a_{j_k})^n = 1$$

for all j , where $1 < j \leq k$. This will be the case precisely when the length of each cycle in the decomposition of σ divides n . The least such n is the least common multiple of the cycle lengths, so the order of σ is equal to the least common multiple of the lengths of the cycles in its cycle decomposition. □

5. 1.6.4

Prove that the multiplicative groups $\mathbb{R} - \{0\}$ and $\mathbb{C} - \{0\}$ are not isomorphic.

Proof. Suppose there exists such an isomorphism $\phi : \mathbb{R} - \{0\} \rightarrow \mathbb{C} - \{0\}$. Then

$$|x| = |\phi(x)| \text{ for all } x \in \mathbb{R} - \{0\}.$$

In both $\mathbb{R} - \{0\}$ and $\mathbb{C} - \{0\}$, $|1| = 1$ and $|-1| = 2$. However, all other elements of $\mathbb{R} - \{0\}$ are of infinite order, whereas, in $\mathbb{C} - \{0\}$, the elements i and $-i$ are both of order 4. Hence, no element of $\mathbb{R} - \{0\}$ may be mapped to i or $-i$ under ϕ , meaning ϕ is not an isomorphism. From this contradiction, we conclude that $\mathbb{R} - \{0\}$ and $\mathbb{C} - \{0\}$ are not isomorphic. \square

6. 1.6.7

Prove that D_8 and Q_8 are not isomorphic.

Proof. We know, from the definition of $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$, that, in Q_8 , the element 1 has order 1, -1 has order 2 and $i, -i, j, -j, k, -k$ have order 4. Now,

$$D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$$

where $r^4 = s^2 = 1$ and $rs = sr^{-1}$. Clearly, the order of s is 2, and we see that

$$(sr)^2 = sr sr = s sr^{-1} r = s^2 = 1,$$

so the element sr has order 2 as well. Hence, D_8 has at least two elements of order 2, whereas Q_8 has only one element of order 2. Since isomorphisms preserve the order of group elements, we can conclude that D_8 and Q_8 are not isomorphic. \square